Information Technology (IT) Incident Reporting Standard

Issue Date: June 1, 2004
Effective Date: June 1, 2004

Number: HHSS-2004-002-D

1.0 Purpose

Security of HHSS Information Technology (IT) resources is paramount to insuring the availability of IT resources and tools and for protecting the privacy and confidentiality of the electronic information created and used to carry out the mission of HHSS. Protecting the security of IT resources relies on the HHSS User community to be vigilant and notify the proper personnel when they witness a security incident that puts HHSS IT resources at risk.

For the purpose of this document a security incident is defined as*: "**The unauthorized use of a HHSS IT Resource or information system, or use of an IT Resource in violation of Nebraska and Federal laws, or HHSS Polices and Standards.***

In the event of a security incident occurring, it is important that all individuals accessing or using HHSS IT resources be aware of their responsibilities and the procedure to report security incidents.

2.0 Scope

This standard applies to employees, contractors, consultants, temporaries, and other workers employed by HHSS including all personnel affiliated with third parties. It is the responsibility of every IT resource user to know these guidelines and act accordingly. This standard applies to all HHSS and State IT resources owned, leased, or supported by HHSS or any outside entity that has signed *Third Party Agreements* with HHSS.

HHSS IT resources referred to in this document include all IT resources as listed in the IT Resources Acceptable Use Standard (HHSS 2004-003-A).

3.0 Standard

This standard provides guidelines for compliance to the Information Technology Security Policy No. HHS-2004-002 and defines guidelines for reporting security incidents.

Since inappropriate activity or activity from unknown sources may result in serious disruption to HHSS services, any suspicious activity witnessed by an individual using an HHSS IT resource, or identified in audit logs must be reported immediately. The appropriate action taken will be dependent upon the type and the critical nature of the incident.

All information gathered and documented in response to a security incident will be held in strictest confidence and only released to appropriate individuals on a "need to know" basis. Only the IS&T Administrator, their agent, the HIPAA PMO, or HHSS Human Resources will have the authority to release information regarding a documented incident.

There are two types of incidents individuals accessing HHSS IT resource must report.

- **Internal Security Incident** –actions or activities by staff and contractors with direct access to HHSS IT resources that bypass security access safeguards or violate HHSS policies.
- **External Security Incident** –an action or activity, by an unknown or unauthorized individual that is a direct threat to the security and availability of HHSS IT resources.

3.1 Internal Security Incident

Any individual accessing HHSS IT resources involved in, or witnessing what they believe to be a security incident or violation of an HHSS Policy, must report the incident to their supervisor immediately. Contractors or business partners are to report the incident to their HHSS business contact. In the absence of the supervisor, incidents may be reported directly to the HIPAA PMO (Health Insurance Portability Accountability Act Program Management Office).

These incidents may include procedural and access issues as well as direct violations of Nebraska law, Federal law, or HHSS IT Policies (see IT Policy Standards: IT Security Standards HHSS 2004-002-(A,B,&C), IT Resource Acceptable Use Standard HHSS 2004-003-A, Software Acceptable Use Standards HHSS-2004-004-(A& B)).

Lost or stolen IT resources such as desktop computers, servers, network equipment, laptop computers, computer disks, portable storage devices, PDAs, printers and computer components are to be reported to the HHSS Help Desk.

Unauthorized changes to system hardware or software without IS&T approval are to be reported to the HHSS Help Desk.

Supervisor/Business Contact Action should include:

- Determine the validity/severity of the incident and report to the appropriate HHSS division contact (Human Resources (HR), HIPAA PMO, HHSS Help Desk) as required.
- Take reasonable and appropriate steps to stop the offending action and to prevent the incident from reoccurring.
- Counsel the individual(s) involved in the incident.
- Provide or arrange for additional training if necessary.
- Request appropriate access as needed.
- Follow normal HR HHSS Policy violation procedures for any incident that involves a personnel action.
- Report repeated incidents by the same individual(s) to the HIPAA PMO.
- Report any unknown or questionable activity involving HHSS IT resources to the HHSS Help Desk.
- When in doubt, report or have the individual involved, report the incident to the HHSS Help Desk.

Help Desk Action should include:

- Create a Trouble Service Request (TSR) and notify the appropriate IS&T technical staff and HIPAA PMO.
- Follow standard procedures in taking reasonable and appropriate steps to stop or contain the offending action.
- For serious or criminal activity notify the HHSS Incident Response Team and begin to preserve any evidence that may be required should a formal civil or criminal investigation be required.

3.2 External Security Incident

Any HHSS IT resource user involved in or who witnesses what they believe to be activity from an unknown or unauthorized source must report the incident to their supervisor and the HHSS Help Desk immediately. Contractors or business partners are to report the incident to their HHSS business contact or if they have access, to the HHSS Help Desk.

Any suspicious activity identified in audit logs or as the result of system audits must be reported immediately to the HHSS Help Desk. When in doubt report all suspicious activity.

Supervisor/Business Contact Action should include:

- Determine the validity/severity of the incident and report to the appropriate HHSS division contact (Human Resources (HR), HIPAA PMO, HHSS Help Desk) as required.
- Take reasonable and appropriate steps to stop the offending action and to prevent the incident from reoccurring.
- Provide or arrange for additional training if necessary.
- Report serious offenses to the appropriate HHSS division contact (Human Resources (HR), HIPAA PMO, or HHSS Help Desk).
- Follow normal HR procedures for any incident that involves an HHSS policy violation or personnel action.
- Report repeated incidents to the HIPAA PMO.
- Follow-up to insure unknown or questionable activity involving HHSS IT resources was reported to the appropriate HHSS division contact (HR, HIPAA PMO, or HHSS Help Desk).

Help Desk Action should include:

- Create a Technical Service Request (TSR) and notify the appropriate IS&T technical staff and HIPAA PMO.
- Follow standard procedures in taking reasonable and appropriate steps to stop or contain the offending action.
- For serious or criminal activity notify the HHSS Incident Response Team and begin to preserve any evidence that may be required should a formal civil or criminal investigation be required.

HIPAA PMO Action should include:

- Document the incident and determine appropriate regulatory reporting requirements.
- Notify appropriate Nebraska and Federal agencies when required by Nebraska or Federal law.
- Counsel the user(s) involved in the incident.
- Follow-up with all parties involved with the reported incident and document the final resolution if required.

4.0 Enforcement

Should a violation of this IT Incident Reporting Standard occur, the individual(s) who committed the violation will be personally liable for their actions or the actions taken by others due to their violation of this standard. Lack of knowledge of or familiarity with the associated policy shall not release an individual from such liability. Any employee found to have violated this standard may be subject to disciplinary action, as defined in the governing policy HHSS 2004-002

5.0 Revision History

HR Legal – 00/00/2004

CCT Approval – 05/27/2004